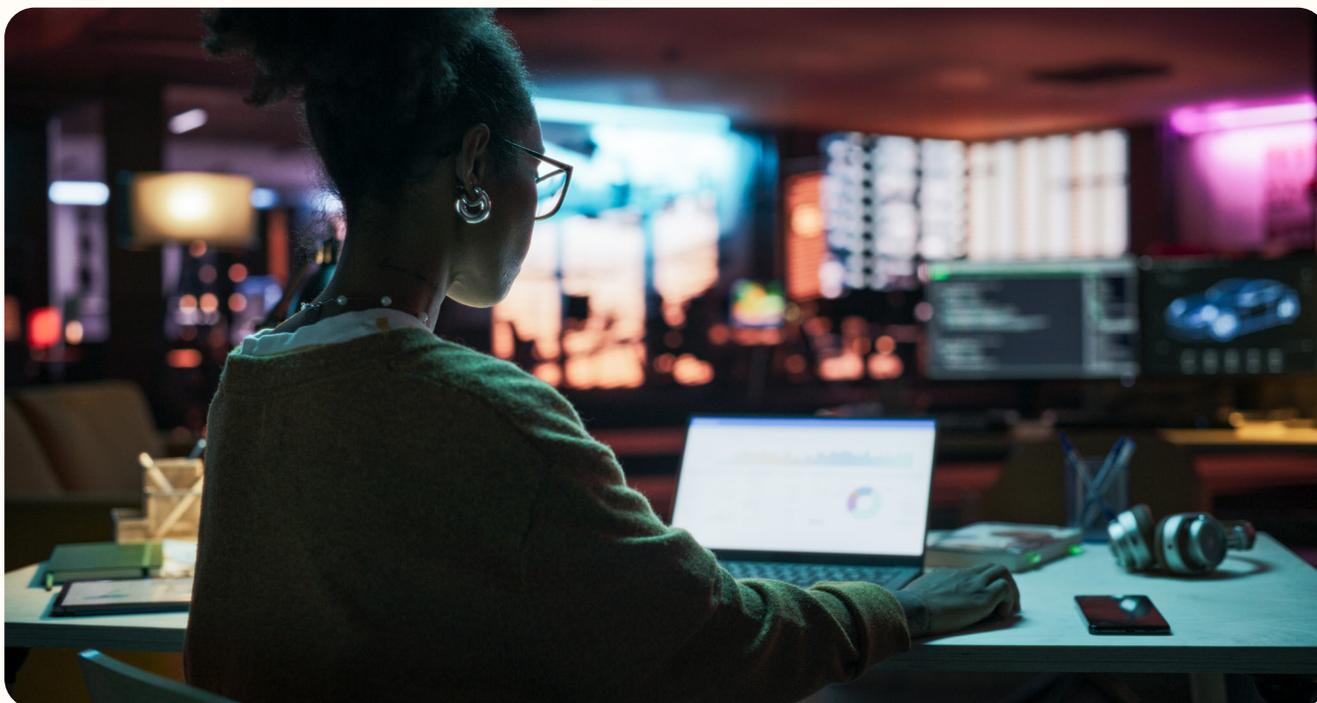

The Only Browser Built to Support Mission

Consumer browsers like Edge and Chrome weren't designed initially as mission support applications. At their core, they are simply vehicles to render web content. In the mission context, at best, they have rudimentary settings that are centrally controllable but no sophisticated policy to protect mission applications, the underlying data, and the personnel in mission departments and agencies.

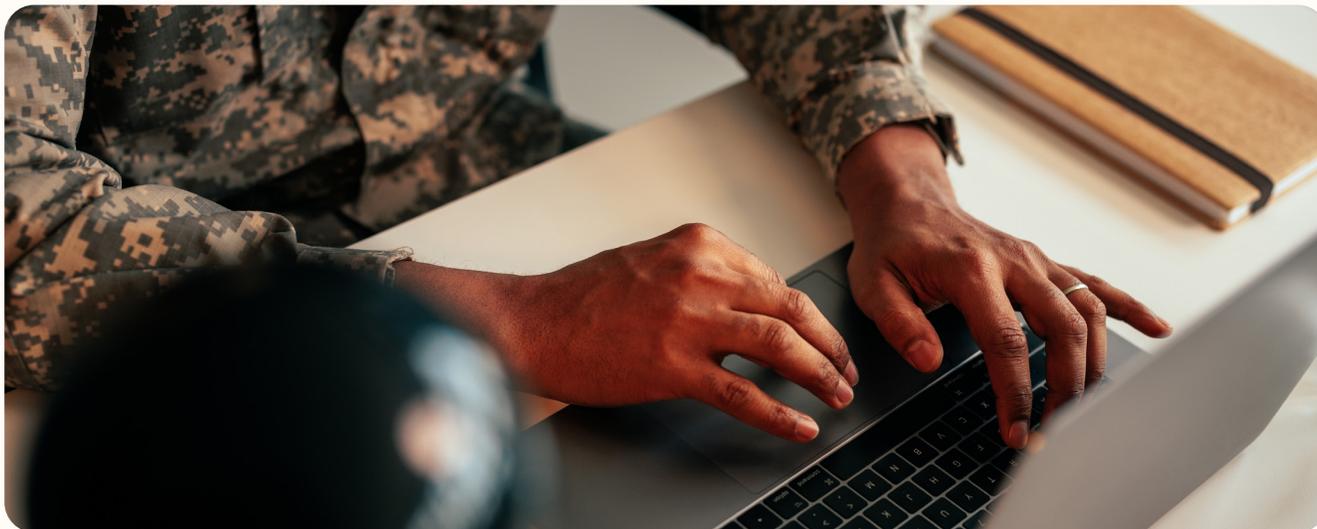
Unsure of this?

Just examine the Joint Regional Security Stack (JRSS) surrounding the typical browsing experience; organizations continue to deploy a complex and expensive series of technologies around these browsers that are challenging to manage and frustrating to work with for Warfighters, civilians, contractors, and mission support alike.

Island, the Enterprise Browser, naturally embeds many of the core needs of mission support into the smooth, familiar browser experience.



Island, The Enterprise Browser



Unlike traditional consumer browsers, Island is contextually aware of the environmental factors it operates within (user, groups, geolocation, network, device awareness, etc). By using such contextual indicators, organizations gain complete control over the last mile, with the ability to govern and audit all browser behavior and customize the browsing experience to support every workflow. Browser activity data is collected and centralized, radically improving the effectiveness of the entire infrastructure. Alternatively, complete user privacy can also be enabled for morale, welfare, and recreation (MWR).

This approach can fill in the missing puzzle pieces of a zero-trust initiative to ensure a natural fit for mission support, mission partner environment data enablement, and a blend of applications that live on the DOD Information Network (DODIN) or in hybrid or public clouds. With Island, security extends everywhere it's needed without getting in the way of mission support:

- Data can be shared securely in mission partner environments (MPEs)
- Software-as-a-Service (SaaS) and DODIN web apps no longer leak data to the endpoint
- Bring Your Own Approved Device (BYOAD) and contract workers get to work without putting data at risk or adding layers of virtualization
- Warfighter, civilian, and contractor credentials are now safe from state-sponsored adversaries, phishing, or inappropriate re-use
- Users are protected from malicious content

Island, the Enterprise Browser, is mission support as it should be: fluid, frictionless, and fundamentally secure.